⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　昭63－124153

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和63年(1988)5月27日
G 06 F 12/14	320	D－7737－5B	

審査請求　未請求　発明の数 1　(全10頁)

㊹発明の名称　記憶情報保護装置

㉑特　願　昭62－232739

㉒出　願　昭62(1987)9月18日

優先権主張　㉜1986年11月5日㉝米国(US)㉛927309

㉒発明者　リーン・デヴィド・コマーフォード　アメリカ合衆国ニューヨーク州カーメル、10ヴアレイ・ロード、アール・デイ　ナンバー1、ボックス191番地

㉒発明者　ピーター・ジエラード・レーダーマン　アメリカ合衆国ニューヨーク州プレゼントヴイル、ベドフオード・ロード224番地

㉑出願人　インターナショナル・ビジネス・マシーンズ・コーポレーション　アメリカ合衆国10504、ニューヨーク州アーモンク(番地なし)

㉔代理人　弁理士　山本　仁朗　外1名

最終頁に続く

明　細　書

1．発明の名称　記憶情報保護装置

2．特許請求の範囲

(1)(a)保護されるべき情報記憶領域を実質的に取囲む包囲体と、

(b)上記包囲体の破壊又は上記領域への侵入などによって状態変化を生じる感知パターンを上記包囲体の中に形成するための手段と、

(c)上記感知パターンに応答し、予定の感知パターンが得られるかを感知するための手段と、

(d)上記感知手段に応答し、予定の感知パターンが得られなかった時に上記記憶情報を破壊するための手段と、

を有する記憶情報保護装置。

(2)上記感知パターン形成手段は上記感知パターンを複数の感知パターンの1つに変化させるための手段を有し、上記感知手段はこの変化された感知パターンに対応する感知パターンが得られるかを検出することを特徴とする記憶情報保護装置。

3．発明の詳細な説明

A．産業上の利用分野

本発明は電子的に記憶される情報のための物理的安全保護技術に関する。

B．従来技術

機械読取り可能な形で入れられているプログラム又はデータを保護するためにコンピュータ業界で取られている伝統的な方法は、コンピュータ設置環境の物理的保護又はこのような保護と何らかの法的保護との組合せを用いるものである。また、許可されない者が不正入手情報を使用できないようにするために暗号化方法も用いられている。パーソナル・コンピュータの領域では、多くの様々なソフトウェア・コピー保護方式が用いられているが、すべてのものはプログラムに組込んだある種のソフトウェア・トラップに基くものであり、徹底した侵害者に対しては有効でない。

米国特許第4471163号はソフトウェア保護機構を開示している。記憶情報の安全保護を図るために、この特許は、プログラム・ロックを装

着する回路板を上下の保護プレートで包囲することを示している。構成要素のための電池電力は保護プレートの内面に取付けた導体を通して供給される。この技術によれば、プリント回路板上の構成要素にアクセスしようとする者は必ず少なくとも一方の保護プレートを動かさねばならず、結果として、電力供給リードを破壊することになる。保護すべき情報を記憶したメモリが電力を必要とするときは、この電力線リードの破壊は侵入者が求めている情報を破壊し、従って情報が保護されることになる。

米国特許第４４７１１６３号の保護機構は、電力線リードが直接取付けられている保護プレート部分を動かした時にしか有効に働かない。このようなプログラム・ロックに何度かアクセスしたことがある徹底した侵害者であれば、保護の程度を知るために何個かの回路板を破壊するとしても、このような保護の裏をかくことは容易にできることである。

情報入手のために装置又は機械設置場所に対してなされる侵入行為がいくつかの段階で行なわれることは想像できることである。

(1) 包囲体又は包囲体及びカバーの取外し

(2) 安全保護センサの位置及び機能の識別

(3) センサを回避して次の保護レベルへ侵入する、

などである。

このような注意深く手順を踏んだ方法を使うと、十分な時間と資源さえあれば、現存する保護システムを打破することが可能である。

C．発明が解決しようとする問題点

本発明の目的は、電子装置に記録される又は記憶される情報に対する安全保護を提供することである。

他の目的は、侵入しようとする者が保護機構の構造に気づいたとしても侵入することが極めて困難な安全保護を提供することである。

D．問題点を解決するための手段

本発明は電子回路に記憶される情報を保護するための、不正操作又は侵入に対して耐性のある情報保護機構を提供するものである。本発明は、情報記憶領域を取囲む包囲体の中に、例えば微細な密な導線を張り巡らしてその導線に所定のパターンで電流を流したり又は光路パターンを形成したりすることにより、包囲体の破壊又はその中への侵入によって状態変化を生じる感知パターンを形成する。感知パターンを検出するため手段が設けられ、包囲体に設定した通りの感知パターンが得られるかが調べられる。破壊又は侵入があった場合は、例えば断線又は短絡などにより感知パターンに変化が生じるから、設定パターンと一致しないパターンが検出される。設定パターンと異なるパターンが検出された時は、これは何らかの侵入を表し、情報を保護するために記憶情報を破壊する。

また、感知パターンを動的に変化させて同様の検出を行なうことができる。感知パターンを予測不可能に変化させることができるから、この方法によれば一層保護の信頼性を高めることができる。

E．実施例

具体的実施例の説明に入る前に、本発明の概要について説明する。

本発明は電子回路に記憶される情報を保護するための、不正操作又は不正侵入に対して耐性のあるパッケージを提供するものである。このパッケージは、保護されるべき電子回路を実質的に取囲む包囲体又は境界スペースを含む。この包囲体に、ある形式のエネルギ、例えば電流、光学的エネルギ、マイクロ波エネルギ、又は無線周波エネルギを供給するためのエネルギ源が設けられる。エネルギ源には、エネルギ分配のための１つ以上の通路よりなるエネルギ分配手段が結合される。分配手段に応答して侵入又は侵入の試みを感知するための感知手段が設けられる。分配手段はエネルギが伝えられる通路のパターン又は通路の形態を変えるための手段を含む。一般にこの手段は分配手段の分配パターンを変える。感知手段は分配手段の分配パターンを知っており、検出された通路パターンを予測パターンと比較することにより侵入を感知する。両パターンの実質的な相違は侵入の証拠となる。感知手段に応答し、侵入があった場

合記憶情報を破壊するための手段が設けられる。

分配手段の動的パターン変更機能を必要としない、本発明の同様のアプリケーションでは、時間の関数としてではなく、異なった保護パッケージの関数として分配手段を変えることができる。即ち、パッケージ1に第1の分配手段を設け、パッケージ2に第2の分配手段を設けるようにすることができる。たとえ同じ分配手段を有するパッケージが多数あったとしても、種々の分配手段がランダムに用いられるから、侵入者はそれがどの分配手段であるかを見極める必要がある。これは容易にはわからないことである。この情報がなければ、他の保護装置の予備知識を盲目的に適用することはできない。

本発明の最も単純なアプリケーションでは、分配手段は変えられない、即ち、時間及び異なるパッケージの両方に関して静的である。しかし本発明は侵入の検出時に被保護電子回路の動作を破壊する手段を含む。

本発明の1つの局面によれば、CMOS RAM又は他の要電力メモリの形で記憶される情報は、複雑な通路をたどる非接触又は絶縁された導体を含む、又はこれで満たされた物理的境界スペースでメモリを包囲することにより、許可されないアクセスから保護される。境界スペースの導体はこの境界スペースへの物理的侵入を電気的に感知するのに用いられる。導体の密度は十分に高くされ、また境界スペースへのいかなる侵入によっても2つの導体間の短絡又は導体の破壊が生じるように十分に脆弱に形成される。導体を支持するのに不透明な包囲材が用いられ、これは侵入時の導体の破壊を容易にする。もし短絡又は導体破壊が生じると、保護された領域内の回路が侵入を感知し、保護されている情報を直ちに破壊する。例えば、境界スペースの導体が揮発性メモリ素子の記憶状態を維持するのに必要な電流を運んでいれば、断線は自動的に記憶情報を消滅させる。しかし導体は揮発性メモリを維持するのに必要な電流を運ぶ必要はなく、単に侵入を感知してこのような揮発性メモリへの電力供給を変えるか電子回路を破壊するのに使用できる。

侵入の感知は電気的である必要はない。電気的導体の代わりに、光学的伝搬路、マイクロ波又は他の無線周波エネルギを使用しうる。

いずれの場合においても、すべての通路を使用して、どれかの通路の乱れによって侵入を判断したり、又は一部の通路を活動状態に、他を非活動状態にし、これらの通路のパターンによって侵入の存在を判断したりすることができる。通路の選択はパッケージ毎に変えることができ、また1つのパッケージ内で動的に変えることもできる。短絡回路又は開放回路によって所定の電圧パターンに乱れを発生させるのではなく、光学伝搬路の乱れを感知して侵入を判断することができる。このような乱れは光学的伝搬路を物理的に乱すことにより生じる。

活動状態及び非活動状態の通路のパターンを動的に変える場合、乱れ又は侵入の存在は、実際の伝導パターンを感知し、これを予期パターンと比較することによって検出される。活動状態の通路はこの通路を開放又は破壊する侵入あるいは乱れによって非活動状態になる。非活動状態の通路は、活動状態の通路への短絡によって、又はそこからの反射エネルギを受取ることによって活動状態になる。パターンを動的に変えると、侵入者は活動状態の通路を単純に迂回することができなくなる。もしそうしようとすると、パターンが変わった時に直ちに侵入が検出される。概して、これらの実施例は、照会/応答の考えに基いている。即ち、活動状態/非活動状態の通路のパターンあるいは条件を設定し、応答を感知し、感知したパターンあるいは条件を最初のステップで設定したパターンあるいは条件と比較し、これらの条件あるいはパターンが一致すれば、保護されている情報を維持する。侵入がなければ、安全保護装置はその応答を予測することができる、即ち、活動状態の通路は活動状態として、その逆はその逆として感知されるはずである。システムの応答が予測応答と異なる時侵入が検出される。

電子的に記憶され、そしてそのように使用され

る情報の場合、その情報又はその誘導物はこれが記憶される形で外界と通信することができる必要がある。典型的にはこれは一連の導電性ピンなどによって行なわれる。パッケージのピン又は端子を介して行なわれる情報アクセスを保護することは本発明の範囲外の論理的安全保護を必要とする。

次に図面を参照して、具体的実施例について説明する。第１図は上壁２１と下壁２２によって形成された包囲体２０を示しており、包囲体２０の中には、保護されるべき情報を記憶する電子回路を装着したカード又はボンド１５が設けられている。壁２１、２２が平坦であれば、包囲体２０を完成するためには側壁が必要であるが、壁２１、２２は平坦である必要はなく、従って側壁は必須ではない。電子回路はコネクタ１６に結合されており、従って情報又はその誘導体は外界と通信できる。本発明の目的は、カード１５に含まれている情報が他のどのような手段によってもアクセス不可能にすることである。電子回路は、簡単な装置例えば数段のシフト・レジスタ及び関連論理回路から一層複雑な装置例えばマイクロコンピュータ又はメイン・フレーム・コンピュータに至るまで種々の複雑度の回路形態を取ることができる。

本発明の最終目標の１つは、カード１５を包囲体２０から取出して、このカードの記憶情報に対してアクセスすることができないようにすることである。即ち、カードを包囲体２０から物理的に取出すことは可能かも知れないが、カードを包囲体２０から取出した時は、カードの中には、侵入者が求めようとした情報が、少なくとも使用可能な形では、含まれていないようにする。

本発明の一実施例によると、包囲体２０は包囲体２０の体積の大部分を満たすか又は少なくともこれを実質的に取囲むように複雑な通路をたどる１つ以上の導体を含む。包囲体２０の体積内の導体は感知手段として用いられる。導体の密度を十分に高くし、導体自体を十分に脆弱にすることにより、体積内への何らかの物体の侵入は導体間の短絡又は導体の開放を生じることになる。導体は比較的脆弱であるのが好ましいが、侵入がない時に装置の完全性を保証ため、導体を支持するための手段が設けられる。支持材は侵入時の開放又は短絡発生の可能性を高め且つ侵入がない時は完全性を維持するように選択される。加えて、本発明の最終目標の１つは、感知手段の特性と似た特性を有する電子装置を作って、この装置を感知手段のある領域と置換し、置換した感知手段の領域を除去してその下側の回路にアクセスし、その中に含まれる情報を取出したりコピーしたり又は変更したりしようとする試みを防止することである。

安価な実施例の場合、包囲体体積はエポキシ・ガラスでよい上側カード２１及び下側カード２２によって包囲される。エポキシ・ガラス・カード２１、２２は内側表面（カード１５の側の表面）に（標準のエッチング・プロセスによって形成された）微細な導電線のパターンを有する。カード２１、２２間の満たされていないスペースは次に黒色のシリコーン充填材（又は他の同様の材料）で満たされる。カード２１、２２の外表面には、保護されるべきカード及びカード内面の導線に対してシールド作用を与える連続した銅（又は他の導電体）の被覆が形成される。この銅被覆はＸ線を用いた内部構造検査を困難にする働きも有する。この感知構成は、保護されるべき情報を含む回路及び情報の維持を制御する回路を含むカード１５と電気的に相互接続される。このような電気的接続は、保護カード２１、２２の内側に配置されカード１５に向けて突出した複数の金属ピンによって与えることができる。これらのピンは製造期間に保護カードのための機械的支持を与えると共に、導電線を破壊せずにカードを取出すことができないようにし、そして何らかの保護対策機能を起動する物理的安全保護を与える。

第２図は、複数の電子回路１５１～１５３を支持しているボンド又はカード１５を示している。カード１５の両側にはカード２１、２２が配置され包囲体を形成している。カード２１、２２はカード１５を実質的に包囲している。カード２１、２２の外面は銅のような導電性被覆２１０、２２０を有する。カード２１、２２の内面には微細な

導体パターン２１５、２２５が付着されている。導体パターン２１５、２２５とカード１５上の回路を相互接続するピン２１６、２２６が選択的に配置されている。この実施例において、カード２１、２２上の導体パターンは複雑な通路をたどって設けられており、そして保護されるべき回路１５１～１５３を含む体積部分を実質的に包囲している。

本発明の一実施例では、ＣＭＯＳ　ＲＡＭチップ（例えば１５１、１５２など）に対する電力は導体２１５、２２５のうちの少なくともいくつかによって供給され、ピン２１６、２２６のうちの少なくともいくつかによってＲＡＭチップに結合される。カード２１、２２あるいはその上の導体２１５、２２５又はピン２１６、２２６が物理的に動かされると、ＲＡＭチップ１５１、１５２などへの電力供給が遮断され、メモリの内容を消滅させるか、少なくとも変更する。

本発明のもう１つの実施例によると、プリント回路導体２１５、２２５及び関連ピン２１６、２２６はメモリ・チップ１５１、１５２などに電力を供給せず、代わりに、ＲＡＭチップへの電力供給を制御するのに用いられる。この実施例では、導体パターン２１５、２２５は感知電流を通されるか又は通されないいくつかの隔離された通路に分割される。これらの通路のすべてが一度に使われる必要はなく、実際に使用される通路パターンは、この目的でつくられそして例えばカード１５上に支持される回路によって動的に選択できる。この回路の例は第３図に示されている。もし実際に電流を運ぶ感知電流供給回路のパターンが電力制御回路（第３図の選択回路及び分配回路）によって設定されたパターンと一致しなければ、回路は電力を遮断し、ＲＡＭチップの記憶内容を破壊する。

第３図に示すように、電池３０１及び／又は他の普通の電源３０２によりＣＭＯＳ　ＲＡＭ１５１および他の回路１５２へ電力が供給される。外部電力が供給される場合に、被保護メモリ又は保護回路の一部でない構成部品の電力ゲート２５２を介して電力を供給するため、普通の電力感知回路３０３が用いられる。これはシステムを使用するためにシステムをオンにする場合に相当する。ＣＭＯＳ　ＲＡＭ１５１は電力ゲート２５１を有し、これはある状態の時に関連ＣＭＯＳ　ＲＡＭ１５１へ電力を供給する。電力ゲート２５１が動作する条件については、次に説明する。

分配回路３０４は感知線３０４－１～３０４－Ｎを選択的に付勢する。これらの感知線の異なるものは異なるパターンの導線２１５、２２５及び関連ピン２１６、２２６によって形成される。すべての感知線を同時に付勢できるが、分配回路によれば一部の感知線のみを付勢することができる。付勢される感知線は時間の関数として変化する。分配回路３０４は、複数の感知線のうちのどれを任意の時間に実際に付勢するかを決める選択回路３０５によって制御される。選択回路３０５は様々な形で実施できる。選択回路は、時間の関数として又は選択回路が応答することができる他の任意のパラメータの関数として、付勢される感知線の選択を動的に変えることができる。比較回路３０６は２組の入力を受取る。１つの入力は選択回路３０５の出力から得られ、これは付勢される分配回路の感知線パターンを識別する。各感知線３０４－１～３０４－ＮはＲ１～ＲＮのような感知抵抗を含み、特定の感知線に電流が流れた時、関連する抵抗に電圧を発生する。電流が流れない感知線では勿論電圧は発生しない。比較回路３０６はもう１つの入力として各感知抵抗からの入力を受取る。比較回路３０６は、電流を流しているべきであると識別された感知線（選択回路３０５から誘導された情報）と実際に電流を流している感知線（抵抗で感知される電圧よって得られる情報）とを比較する。２つのパターンが一致する時にのみ電力ゲート２５１は電力をＲＡＭ１５１へ供給する。このように比較回路３０６は、電流を流すべきすべての感知線が電流を流しており（従って、例えば侵入によって導体パターンに開放回路がつくられていないことを保証し）、また電流を流すべきでない感知線が電流を流していないこと（侵

入の結果、電流を流すべき、感知線と電流を流すべきでない感知線との間に短絡が生じたり、又は侵入者が故意に橋絡したりしていないこと）を判定することができる。２つのパターンが一致しない時電力ゲート２５１はＲＡＭ１５１への電力供給を遮断する。また、不一致時に起動回路１５３を付勢して電源回路の遮断あるいは記憶の消去又は電子回路の破壊を開始することができる。

第３図の装置は付勢される電流通路感知パターンと付勢されない電流通路感知パターンを動的に変える選択回路３０５を含むものとしているが、選択回路３０５が動的でなく、時間に関して静止しているような不正操作防止パッケージを提供することも本発明の範囲に含まれる。より簡単な実施例では、個々のパッケージが異なる選択回路３０５を持つことができる。従って、第１のパッケージでは、第１の選択回路３０５が第１のパターンの付勢／減勢通路を持ち、第２のパッケージでは、第２の選択回路３０５が異なる第２のパターンの付勢／減勢通路を持つようにすることができる。任意のパッケージでは付勢される通路と付勢されない通路のパターンは一定であるが、あるパッケージに侵入しようとした時に得た情報を使って別のパッケージに侵入することはできない。同じ電流通路パターンを有するパッケージが何千とあったとしても、通路パターンは種々に変えることができるから、この方法でも十分な不正防止効果を得ることができる。

一層簡単な実施例は、選択回路３０５を静的にし且つ、すべてのパッケージに同じ電流通路パターンを持たせるものである。

第４図及第５図は、分配及び感知のための代替構成を示している。第４図は１対のスイッチ・バンク４２０、４４０により、感知線４６２、４６４、４６６、４６８の位置を制御する回路を示している。スイッチ・バンク内のスイッチ４２２～４２８、４４２～４４８の位置は選択発生器４８０によって制御される。実際の例では、スイッチはＣＭＯＳアナログ・ゲートのような電子装置であり、選択発生器はスイッチ位置を制御するすべての選択が有効な感知パターンを与えるように設計される。これはすべての有用な感知パターンを記録するか又はアルゴリズムで発生することによって行なうことができる。いずれの場合でもこのような発生方法はディジタル設計の熟練者には明らかなことである。感知線を効果的なパターンで接続した場合は、完全な回路が形成され、電流源４１０からの電流が内部ジャンパ４１２、負荷抵抗４１４及び電流検出器４１６を介して流れる。実際の例では４本よりも多数の感知線を使用することができることは勿論である。また、感知線の長さは情報を含む回路及び関連回路を包囲するスペースを不正操作検出部４６０で実質的に満たしうるように選ばれることも理解されよう。更に、種々の回路要素（電流源４１０、ジャンパ４１２、負荷４１４、電流検出器４１６）は、任意の使用可能な信号源、検出器を含む様々な整合性のある構成要素で置変することができる。

第５Ａ図～第５Ｃ図は不正操作検出部４６０のある大きな部分を、これと同じ電気特性を有する回路で置換することによってこの部分を取外そうとする侵入の際に起りうる状態を示している。第５Ａ図の不正操作検出部４６０は第４図と同じく構成されている。侵入者は導線を封入している充填材を注意深く除去して、離れた点Ａ、Ｂ、Ｃ、Ｄを露出させたものとしている。普通の電子技術によれば、これらの４つの点を含む回路部分を適当な値の外部抵抗５５で置換しうることがわかる。侵入者は電流検出器４１６で検出できないような短い時間で第５Ｂ図のように抵抗を置換するかも知れない。図示の電流検出器は、後述するように、長い放電時定数を有する普通の設計の１トランジスタ・インバータよりなり、従ってスイッチ・バンクの状態変化の際の一時的電流不在が侵入として誤解釈されて、これにより被保護情報が消去されることはない。第５Ｃ図はスイッチ・バンク４２０、４４０が状態変化（任意の時間に起りうる）した後の回路構成を示している。この新しい構成では、外部抵抗５５は取外された検出器領域に対する有効な置換手段として機能せず、従って電流

検出器の電流不在によって侵入が検出され、これは出力線６３の状態変化によって示される。

このような置換による侵入を検出する本発明は、侵入者に対し、時間がかかり、骨が折れ、万が一の失敗も許されない厄介な作業を強いるという効果があり、しかもこのような侵入の試みは、不正操作検出器を適正に構成するか又は置換により生じる個々の線の電気的特性の累積的変化を検出できる普通の測定装置と共に本発明のシステムを使用することにより防止することができる。

電流検出器４１６において、キャパシタ５９が充電された後にキャパシタの両端に現れる定常状態電位は抵抗５７及び４１４によって形成される分圧器、電流源４１０の電位、並びにトランジスタ６１のエミッタ・ベース接合によって設定される。この回路で用いられる構成要素の値は、この電位が、トランジスタ６１のエミッタ・ベース接合を介して電流を流しトランジスタ６１を強く導通させるのに十分になるように選ばれる。電流検出器の電圧を分割する機能に加えて、抵抗５７は、トランジスタ６１のエミッタ・ベース接合、キャパシタ５９及び抵抗５７よりなるＲＣ回路の放電時定数が十分に長くなり、そしてスイッチ・バンク４２０、４４０による回路の再構成の際に電流検出器４１６が残りの回路から短時間切り離される時でもトランジスタ６１が強く導通し続けるように選択される。トランジスタ６１が強く導通した状態にある結果として、コレクタに接続された状態出力端子６３の電位は大地電位に近ずく。この回路を普通のＴＴＬ論理回路に接続すれば、出力端子の状態は、論理回路により論理レベル"０"として解釈される。この状態出力を用いる回路はこのレベルを、無不正操作状態を示すものとして解釈する。第５Ｃ図のように、回路の流れる電流がスイッチング時間よりも長い間遮断されると、キャパシタ５９の放電のため、トランジスタ６１を導通状態に保つのに必要な電流を供給できなくなる。これが生じると、状態出力６３は大地電位から離れる。この状態変化は、普通のＴＴＬ回路により論理レベル"１"として解釈され、不正操作の検出を表わす。この回路は通電圧状態の検出又は回路抵抗変化の検出のような他の検出技術を含むように容易に変更できる。この回路はこのようなシステムの動作原理を例示するためのものにすぎない。

カードの側面からプローグを挿入してカードの安全保護を破ろうとしても、充填材３０を通して正確にプローグを差し込むのが難しいこと並びにその通路の長さ及び狭さの点で厳しい制限があることから見て、そのようにするのは非常に難しい。代替的には、通路部分を何らかの感知手段で覆うこともできる。Ｘ線又は音波のような案内補助手段を用いた位置付けをするのは不可能である。というのは、ＲＡＭはＸ線に敏感であり、またシリコーンを通して音波像をつくるのは難しいからである。

テクスチャ構造の表面に導電線を配置することにより、機械的シリング又はプラズマ・エッチングが困難になる。即ち、単一の電流通路の異なる部分が異なる水平区分に存在するようにランダムに高さを変えて導線を配置することにより、侵入者は機械的シリング又はプラズマ・エッチングを利用できなくなる。

電気的には同じ機能でも異なった導体配置構造を有するいくつかの設計を用いれば、あるカードを分解することによって得られる知識が他のカードに対してはあまり役立たないことになるから、相当の侵入防止効果が得られる。

第２図及び第３図の実施例を光学系で実施する場合、電源は光源で置換され、感知線２１５、２２５は自由光路で置換され、分配機能は光走査で置換され、抵抗Ｒ１～ＲＮは感光性装置で置換される。侵入の検出は、侵入により光路が遮断されて特定の感光性装置で光エネルギが受信されなくなることによって又は、侵入により別の感光性装置に光エネルギ（例えば侵入物体による反射光）が与えられることによって行なわれる。

光エネルギに対して自由空間伝搬路を与えるためには、不透明な充填材を除去するか又は光チャンネルを形成する必要がある。自由な又はガイド

付きの光伝搬の場合は夫々が付属の感光性ダイオードを有する複数の光路を単一の光源（例えばレーザ・ダイオード）で駆動することができる。付勢される光路／付勢されない光路は光源と選択された通路との間の連路を制御することにより、又は光源を再方向づけすることにより選択できる。代替的には、複数の光源を選択的に付勢／滅勢できる。

F．発明の効果

本発明によれば、情報記憶領域を取囲む包囲体の破壊又は異物の侵入を確実に検出して情報を破壊することができるから、電子装置を破壊して情報記憶部を取出そうとしたりプローブなどにより情報を不正入手しようとしたりする物理的な侵入行為から記憶情報を保護することができる。

4．図面の簡単な説明

第1図は、本発明によるパッケージを示す図である。

第2図は、第1図のパッケージの断面図である。

第3図は、本発明の実施例の回路図である。

第4図は、分配及び感知システムの別の構成例を示した図である。

第5A図、第5B図及び第5C図は、侵入時に起りうる状態を例示した図である。

出願人　インターナショナル・ビジネス・マシーンズ・コーポレーション

代理人　弁理士　山　本　仁　朗

（外1名）

FIG. 1

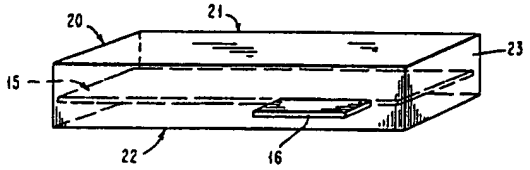


FIG. 2

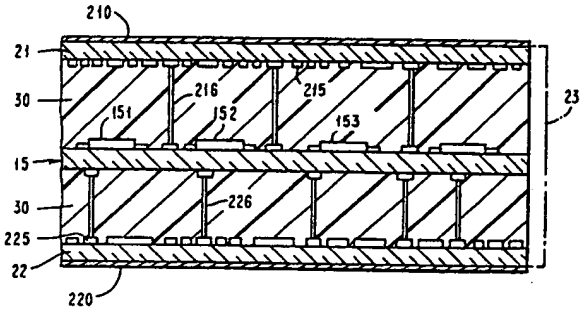


FIG.5A

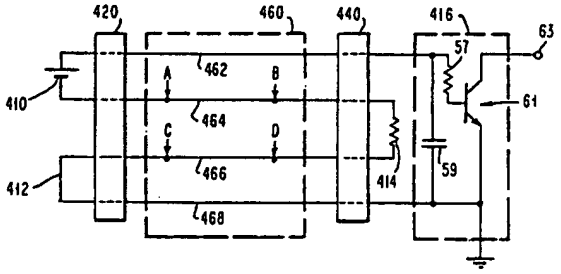


FIG. 5B

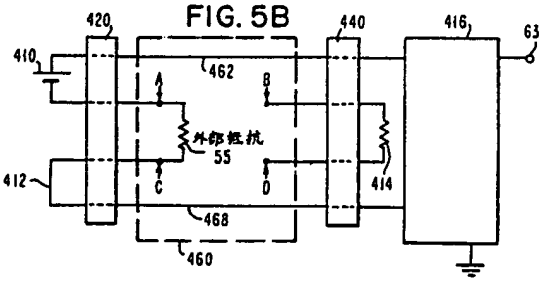


FIG. 3

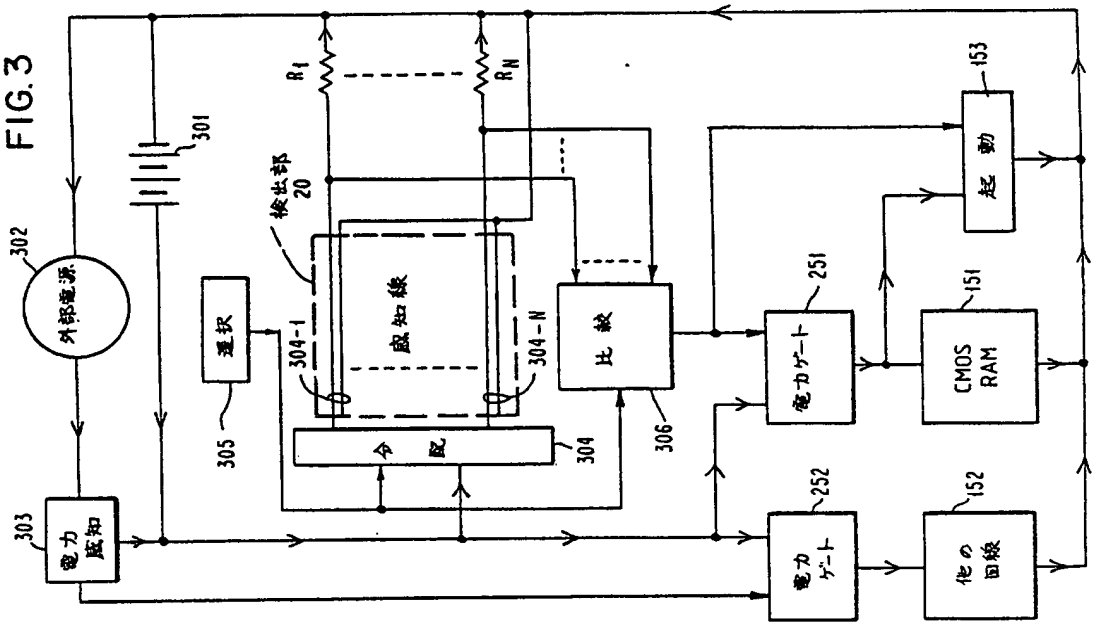

外部電源
302
301
303
電力感知
検出部
20
R_1
R_N
304-1
304-N
感知線
304
分配
305
選択
306
比較
251
電力ゲート
252
電力ゲート
151
CMOS RAM
152
他の回路
153
起動

FIG. 4

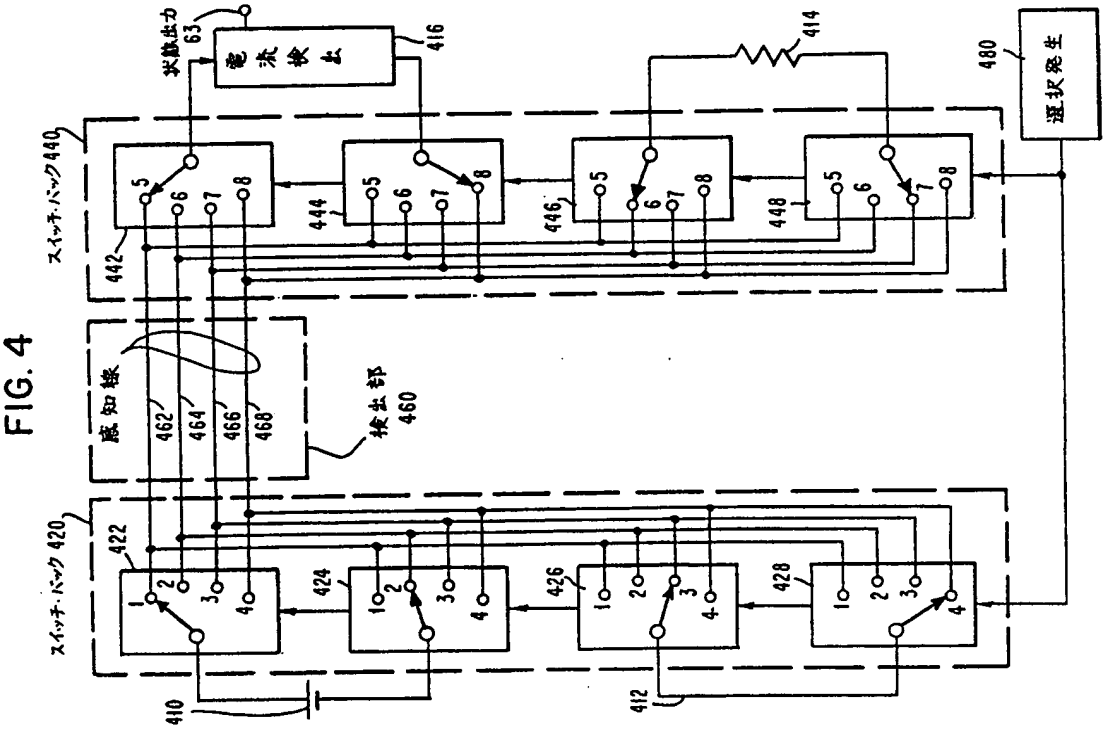
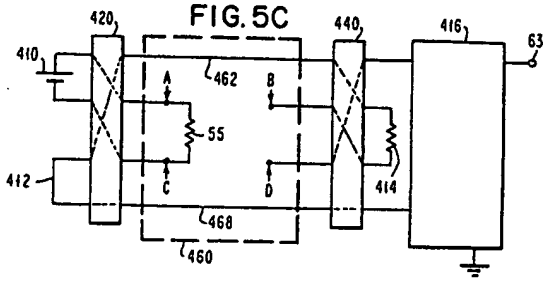

状態出力
63
電流検出
416
414
480
選択発生
スイッチバンク440
442
444
446
448
感知線
462
464
466
468
検出部
460
スイッチバンク420
422
424
426
428
410
412

FIG. 5C



第1頁の続き

⑫発　明　者	ローレンス・アーウイン・リーヴイ	アメリカ合衆国ニューヨーク州ヨークタウン・ハイツ、メドウクレスト・コート2977番地
⑫発　明　者	ステイヴ・リチャード・ホワイト	アメリカ合衆国ニューヨーク州ニューヨーク、アパートメント33、パーク・アヴエニユー7番地